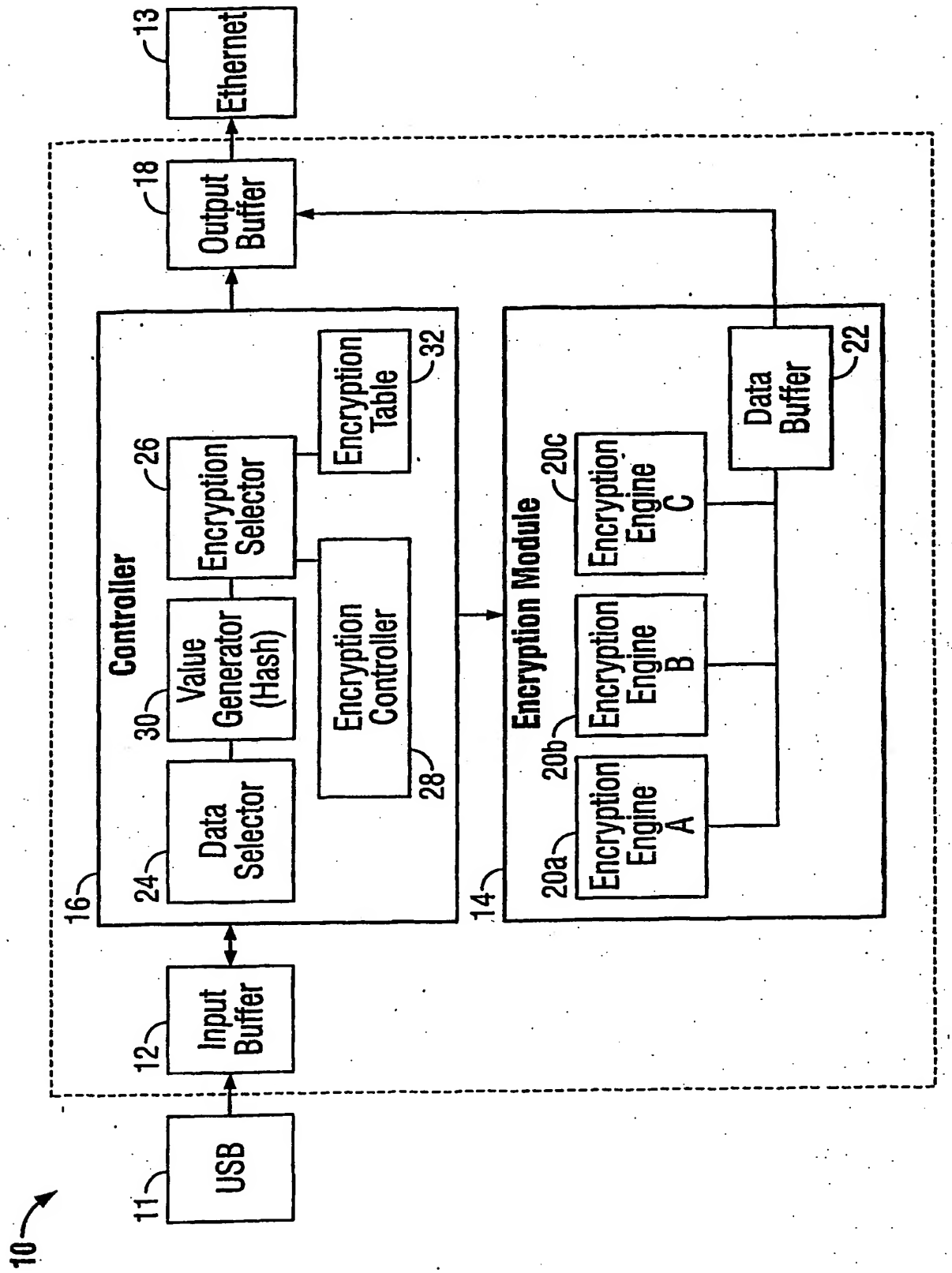
10
11
USB
12
Input Buffer
13
Ethernet
14
Encryption Module
16
Controller
18
Output Buffer
20a
Encryption Engine A
20b
Encryption Engine B
20c
Encryption Engine C
22
Data Buffer
24
Data Selector
26
Encryption Selector
28
Encryption Controller
30
Value Generator (Hash)
32
Encryption Table

FIG. 1A

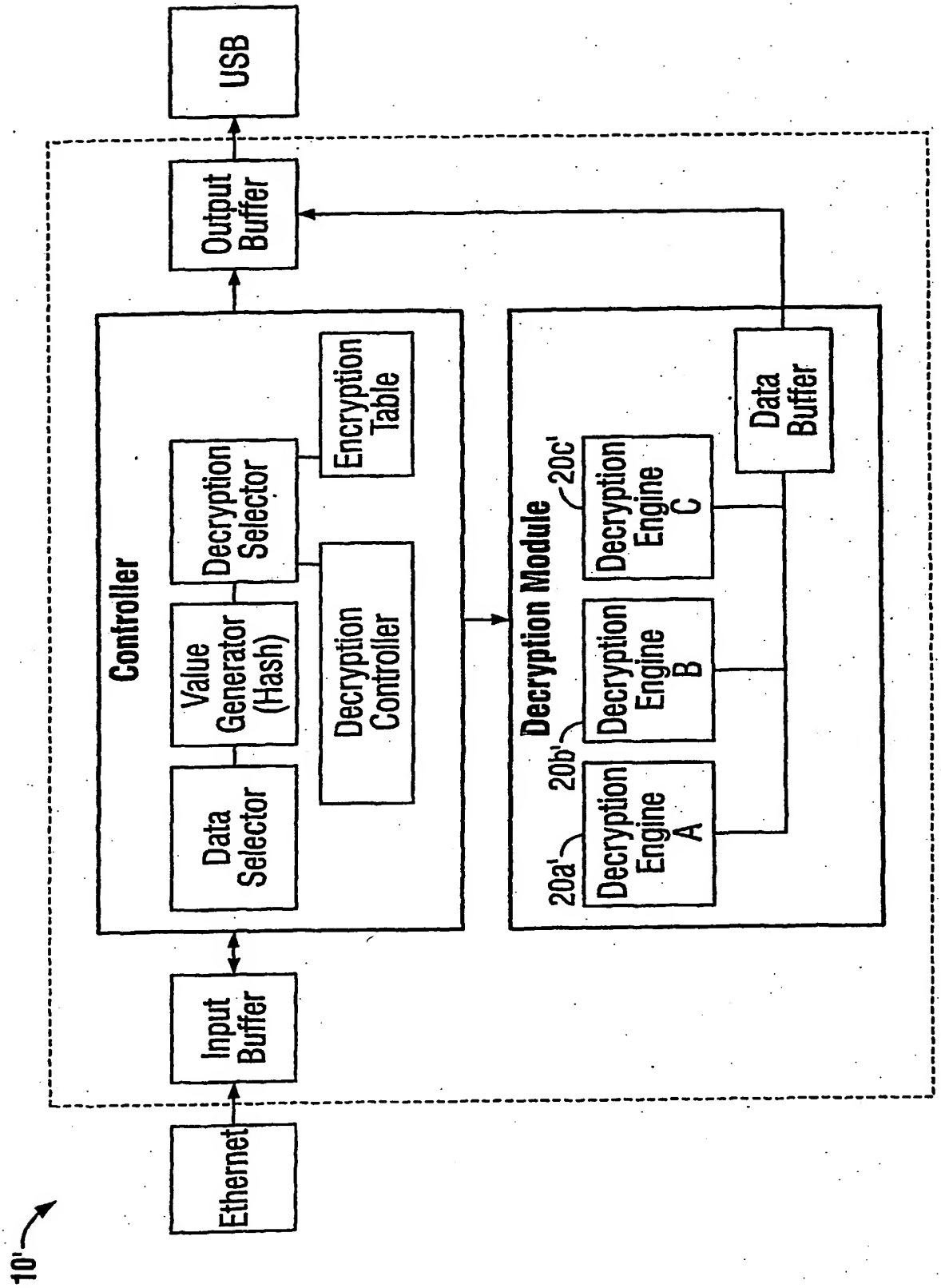
10'
Ethernet
Input Buffer
Controller
Data Selector
Value Generator (Hash)
Decryption Selector
Encryption Table
Decryption Controller
Output Buffer
USB
Decryption Module
20a'
Decryption Engine A
20b'
Decryption Engine B
20c'
Decryption Engine C
Data Buffer

FIG. 1B

32

| Index | Encryption Type | Key | Initial Vector |
|---|---|---|---|
| 0 | 3 DES | Key 1 | 5 |
| 1 | AES | Key 2 | 2 |
| 2 | 3 DES | Key 3 | 7 |
| 3 | IDEA | Key 4 | 8 |
| 4 | AES | Key 5 | 3 |
| ⋮ | ⋮ | ⋮ | ⋮ |

FIG. 2

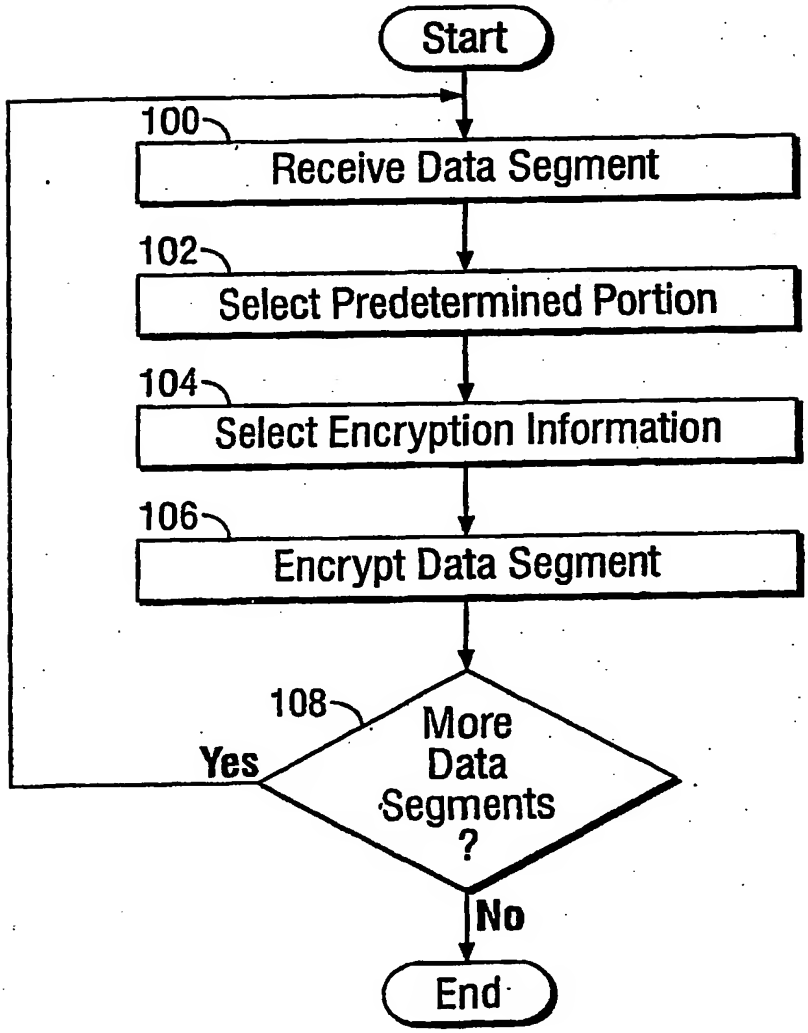


FIG. 3

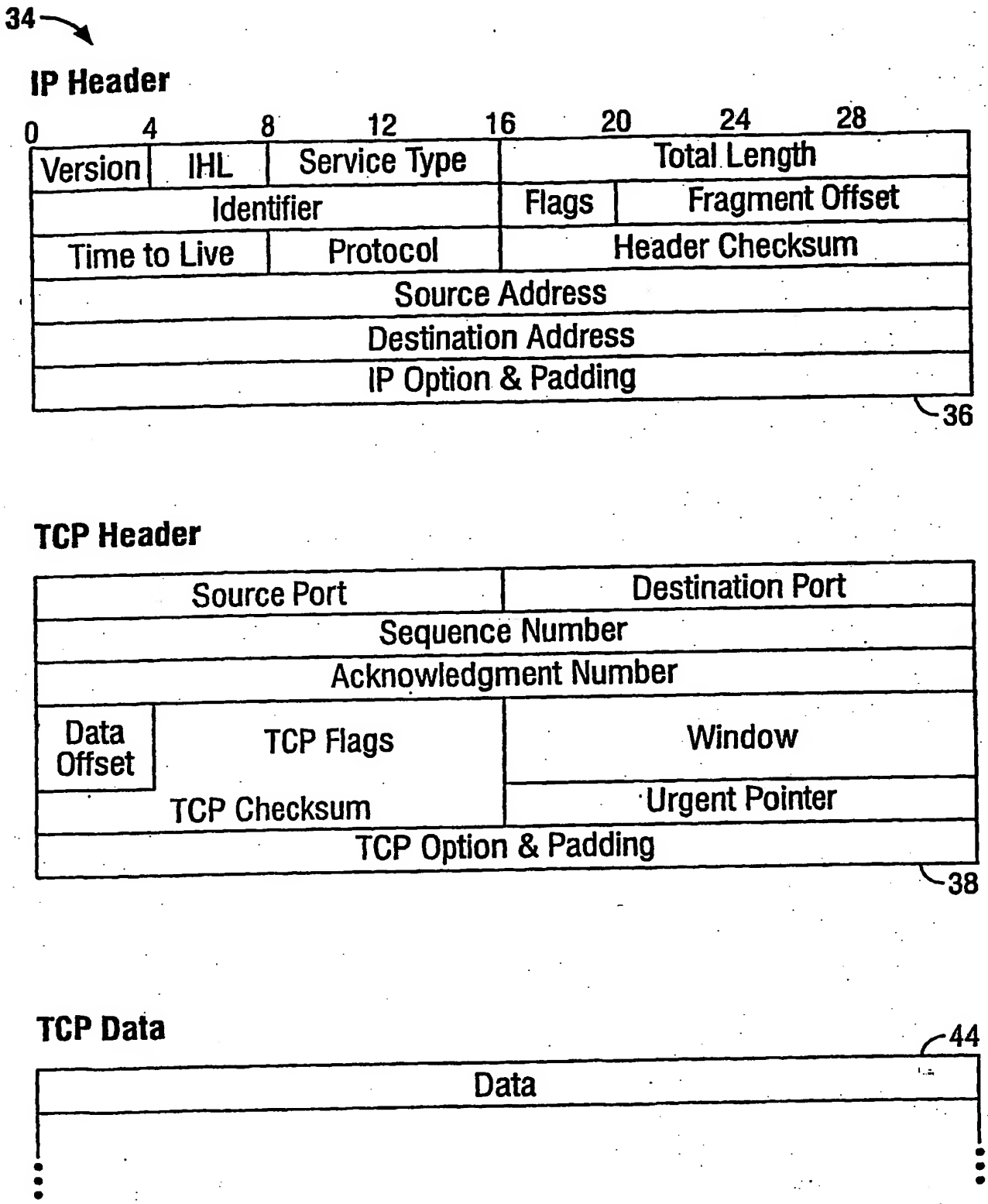
34
IP Header
0
4
8
12
16
20
24
28
Version
IHL
Service Type
Total Length
Identifier
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
IP Option & Padding
36
TCP Header
Source Port
Destination Port
Sequence Number
Acknowledgment Number
Data Offset
TCP Flags
Window
TCP Checksum
Urgent Pointer
TCP Option & Padding
38
TCP Data
44
Data

FIG. 4

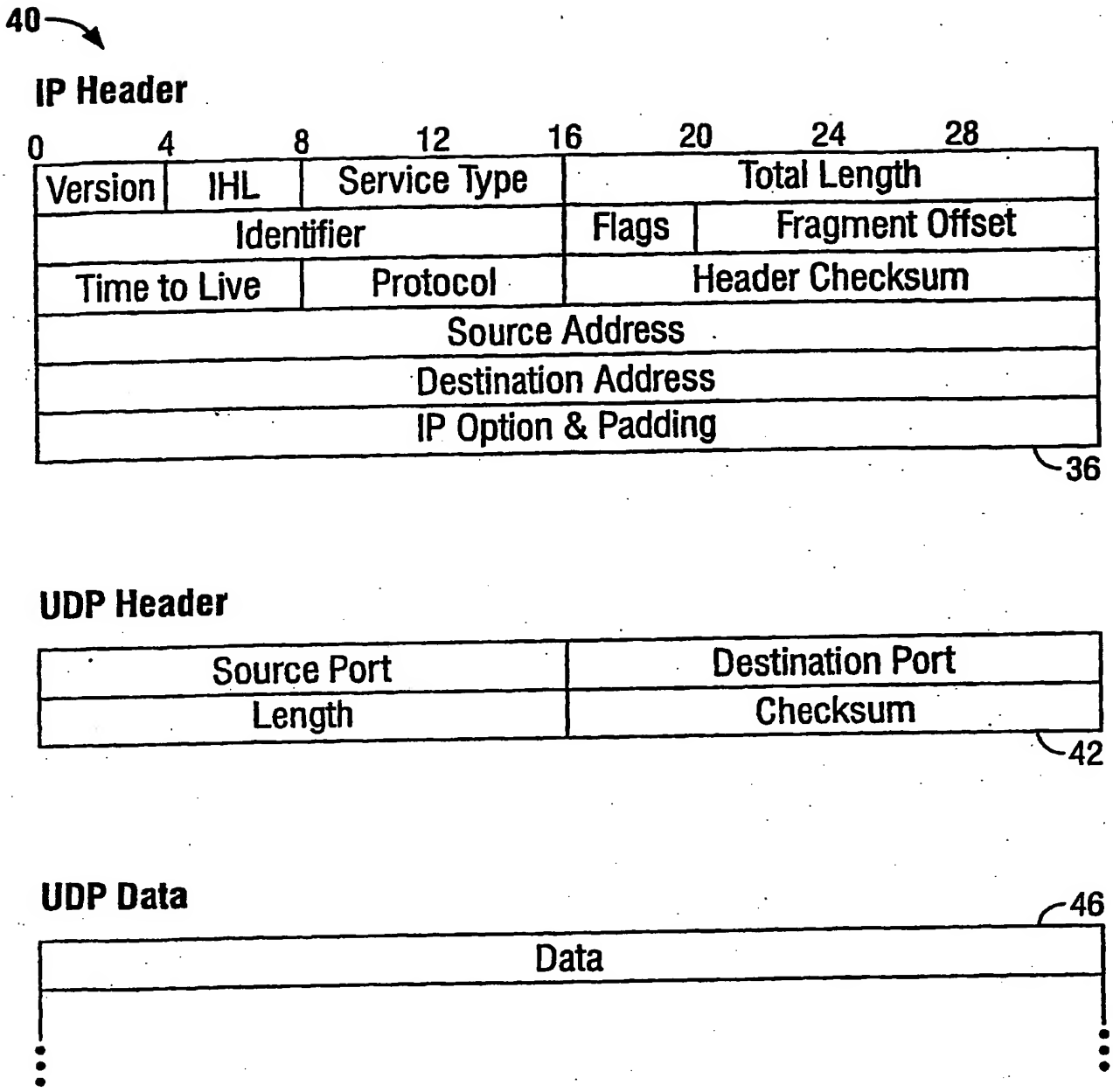
40
IP Header
0
4
8
12
16
20
24
28
Version
IHL
Service Type
Total Length
Identifier
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
IP Option & Padding
36
UDP Header
Source Port
Destination Port
Length
Checksum
42
UDP Data
46
Data

FIG. 5

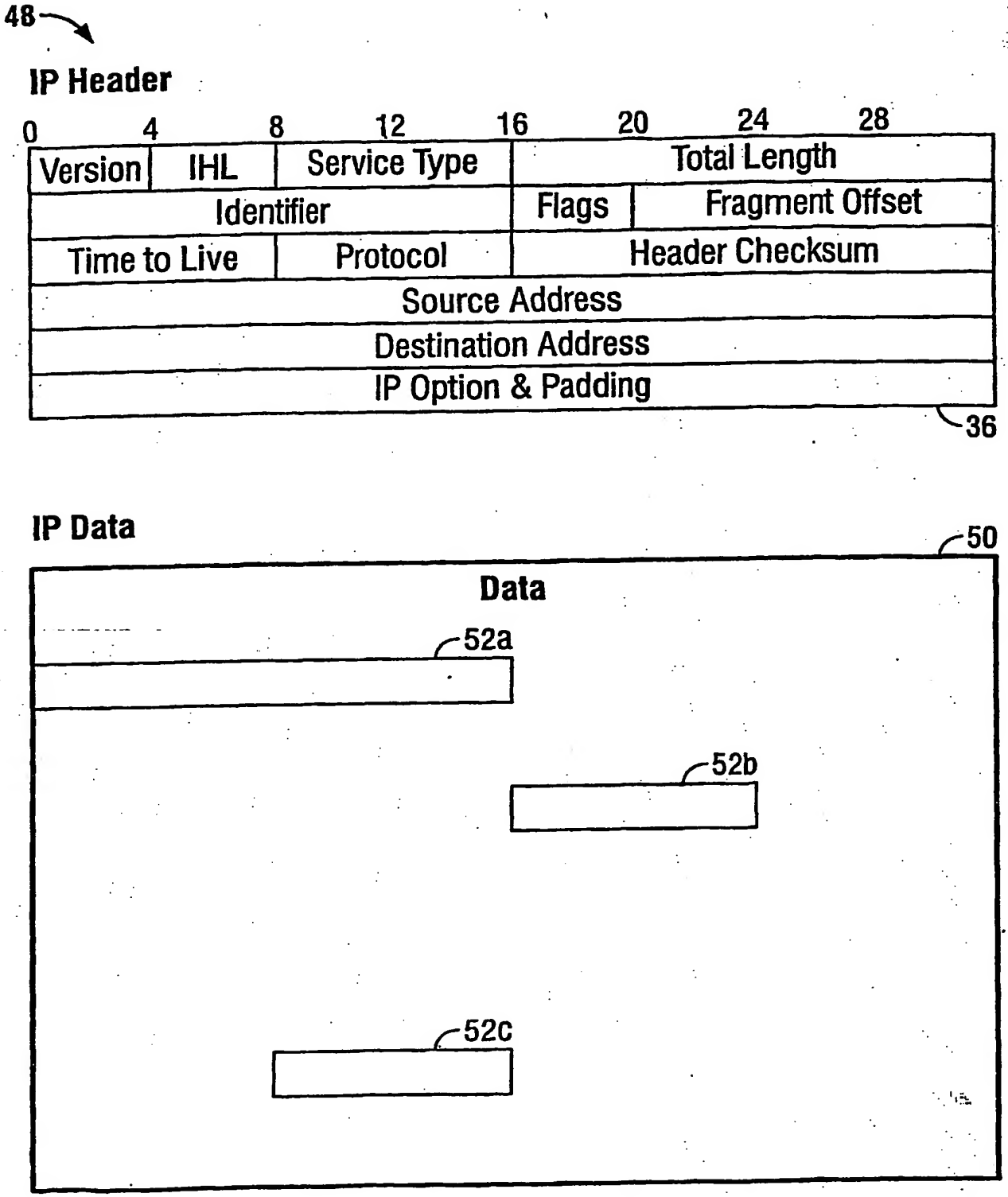
48
IP Header
0
4
8
12
16
20
24
28
Version
IHL
Service Type
Total Length
Identifier
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
IP Option & Padding
36
IP Data
50
Data
52a
52b
52c

FIG. 6

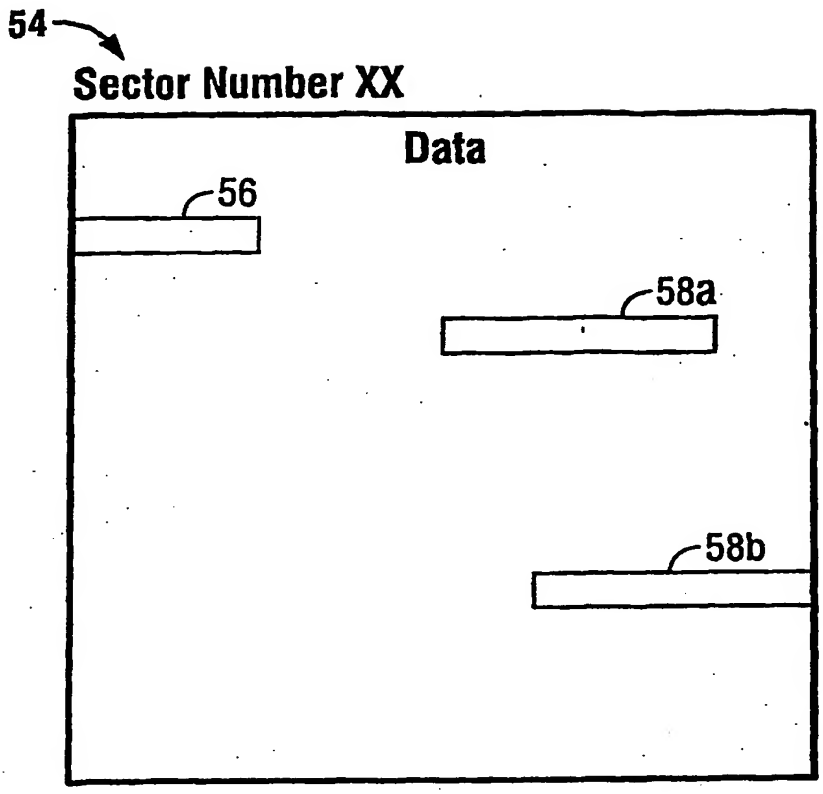
54
Sector Number XX
Data
56
58a
58b

FIG. 7

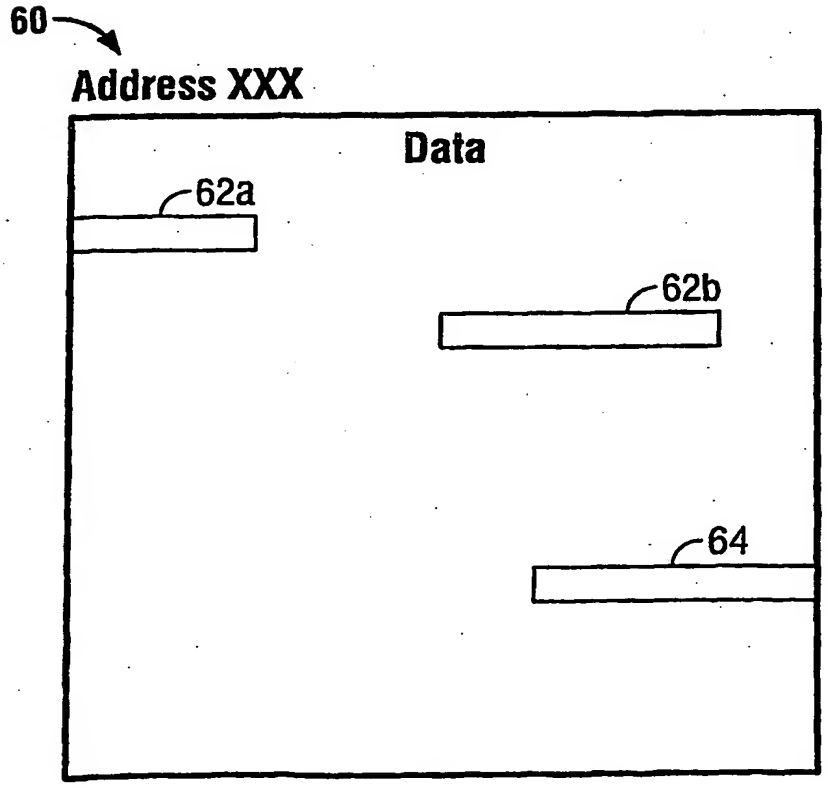
60
Address XXX
Data
62a
62b
64

FIG. 8

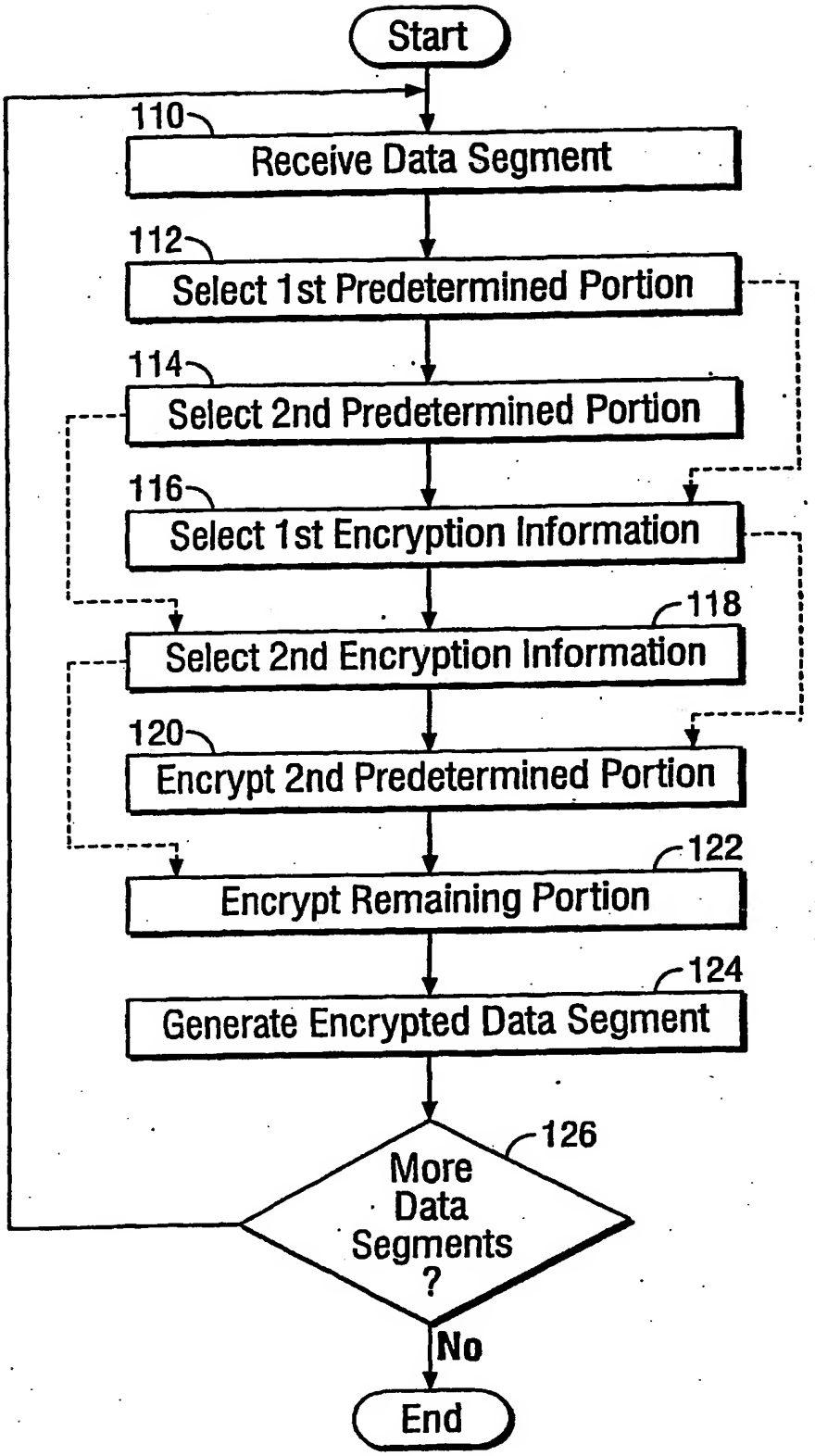
Start
110
Receive Data Segment
112
Select 1st Predetermined Portion
114
Select 2nd Predetermined Portion
116
Select 1st Encryption Information
118
Select 2nd Encryption Information
120
Encrypt 2nd Predetermined Portion
122
Encrypt Remaining Portion
124
Generate Encrypted Data Segment
126
More Data Segments ?
No
End

FIG. 9

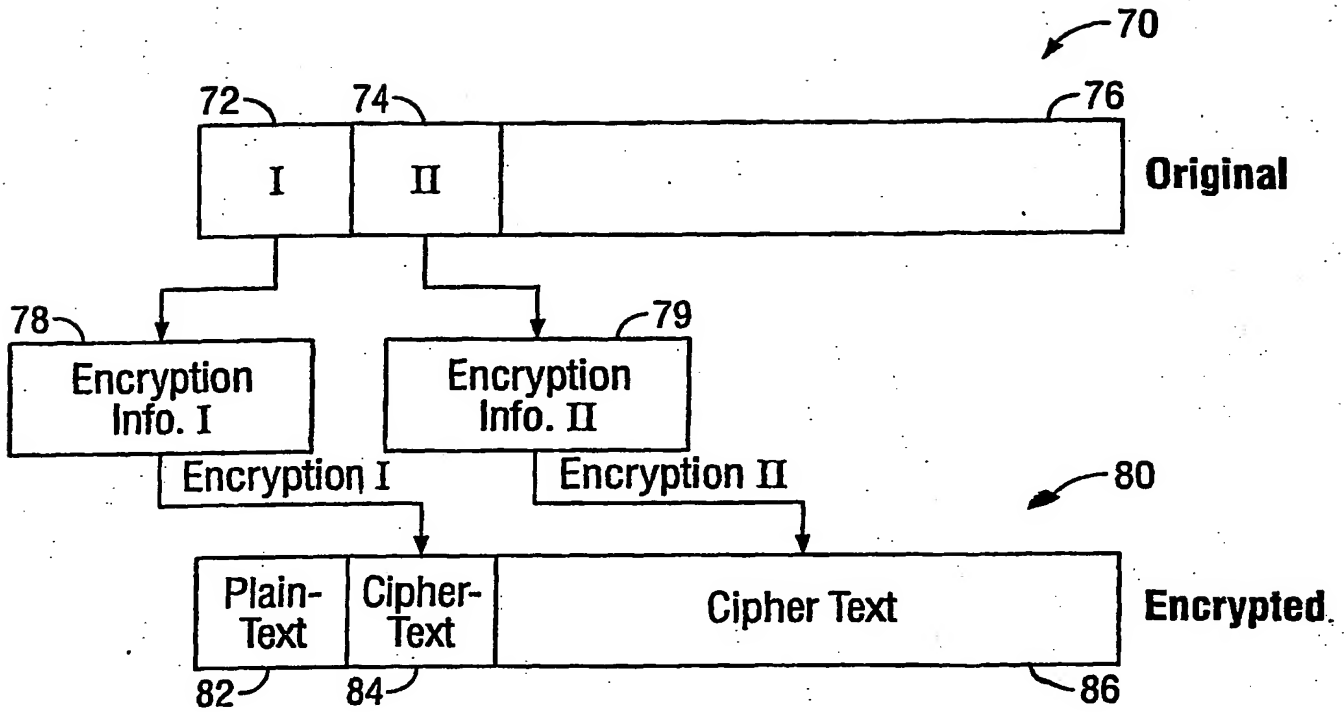
70
72
74
76
I
II
Original
78
79
Encryption Info. I
Encryption Info. II
Encryption I
Encryption II
80
Plain-Text
Cipher-Text
Cipher Text
Encrypted
82
84
86

FIG. 10

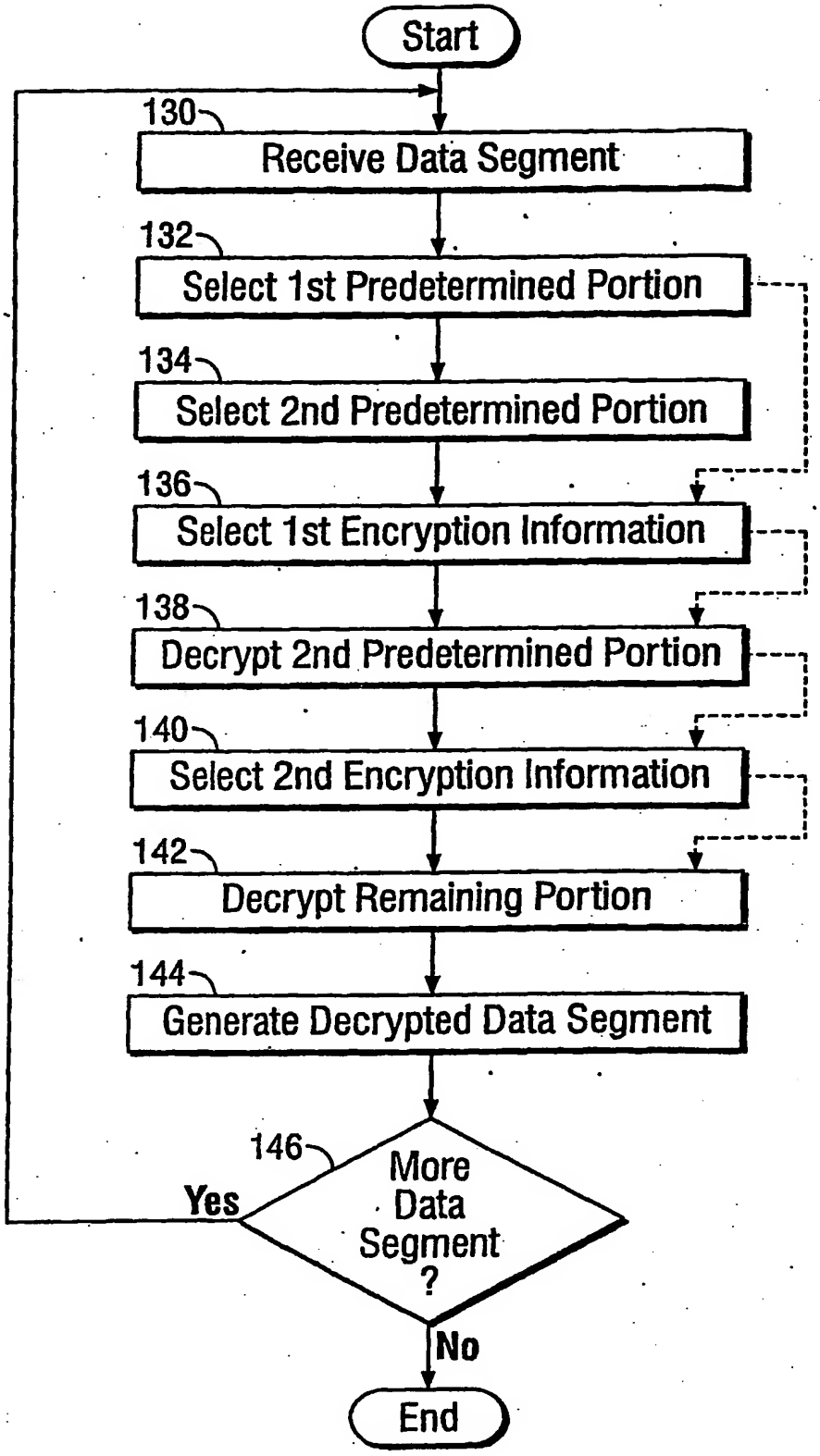
Start
130
Receive Data Segment
132
Select 1st Predetermined Portion
134
Select 2nd Predetermined Portion
136
Select 1st Encryption Information
138
Decrypt 2nd Predetermined Portion
140
Select 2nd Encryption Information
142
Decrypt Remaining Portion
144
Generate Decrypted Data Segment
146
More Data Segment ?
Yes
No
End

FIG. 11

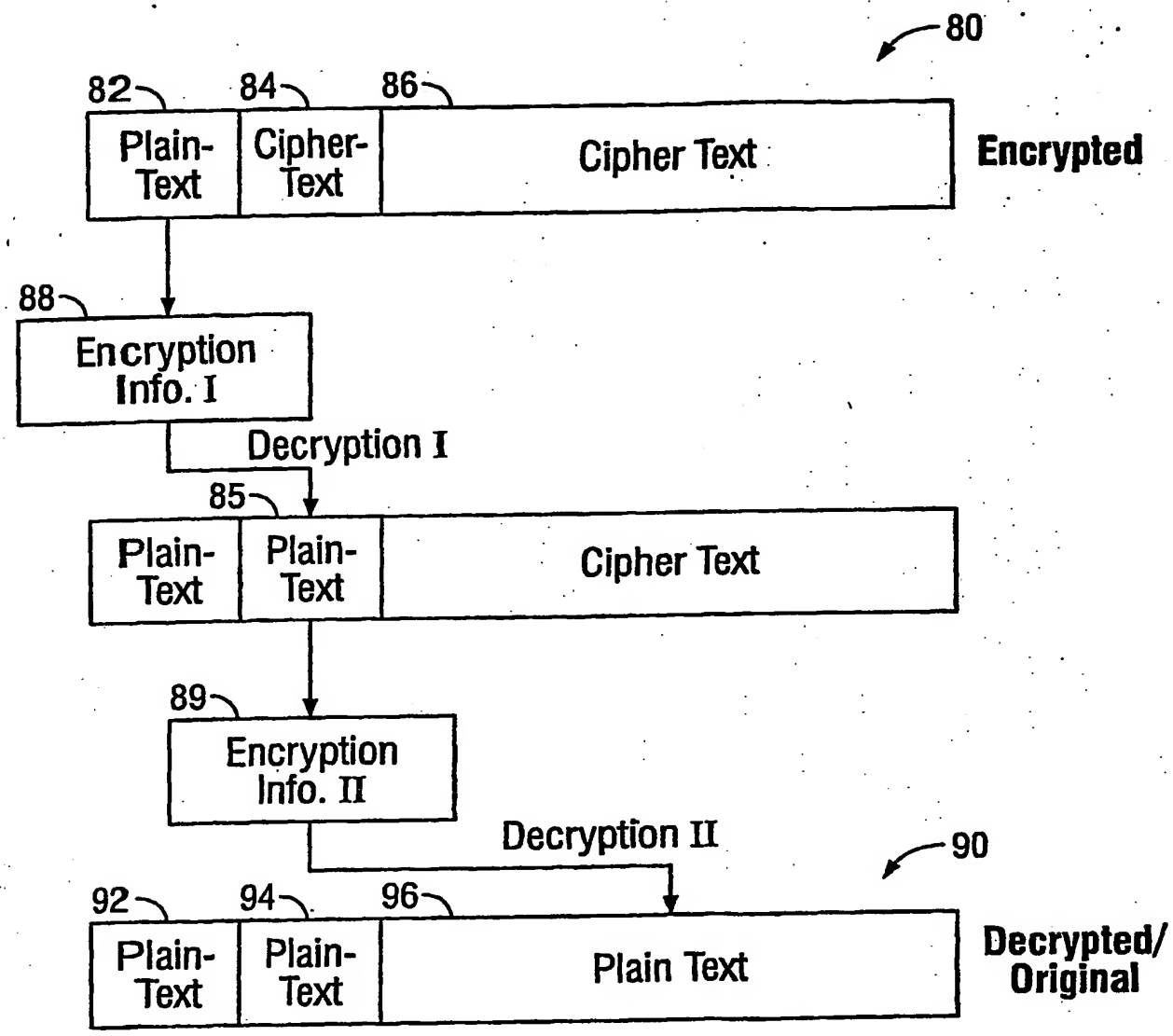
80
82
84
86
Plain-Text
Cipher-Text
Cipher Text
Encrypted
88
Encryption Info. I
Decryption I
85
Plain-Text
Plain-Text
Cipher Text
89
Encryption Info. II
Decryption II
90
92
94
96
Plain-Text
Plain-Text
Plain Text
Decrypted/ Original

FIG. 12

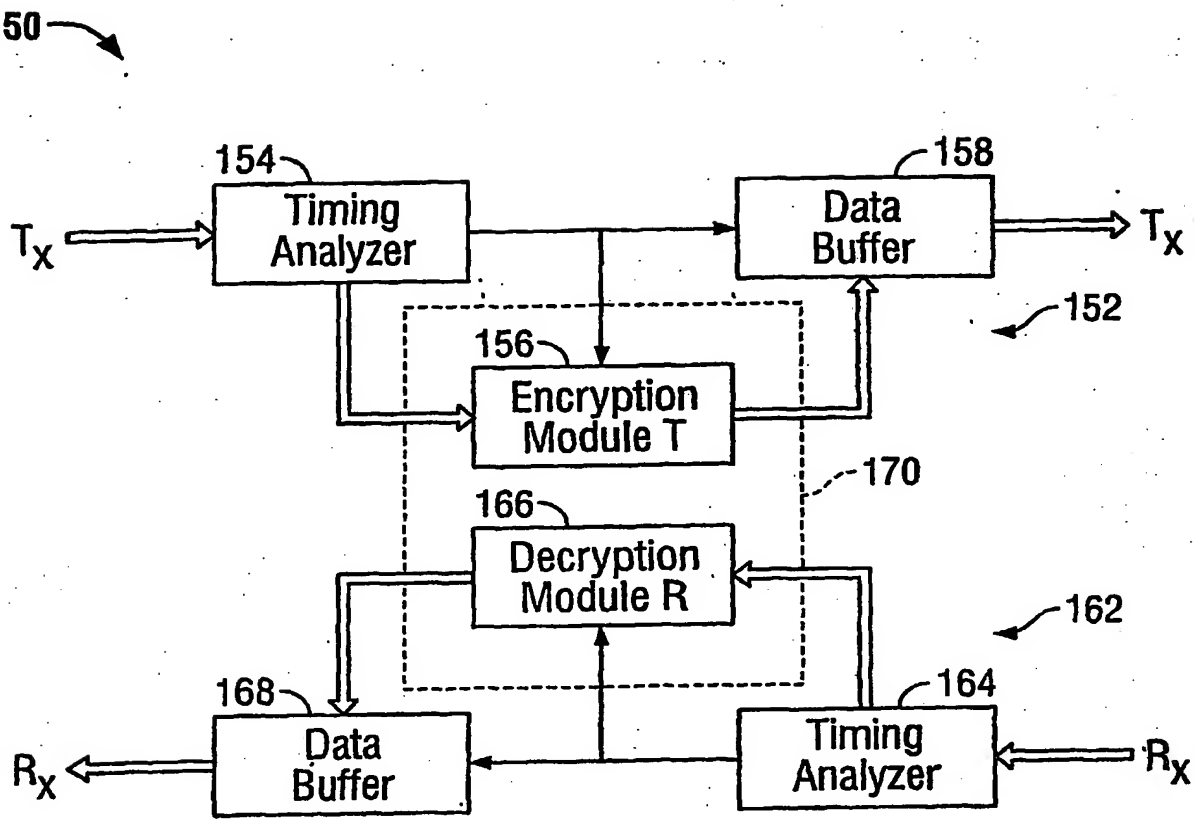
150
154
Timing Analyzer
158
Data Buffer
$T_X$
$T_X$
152
156
Encryption Module T
170
166
Decryption Module R
162
168
Data Buffer
164
Timing Analyzer
$R_X$
$R_X$

FIG. 13

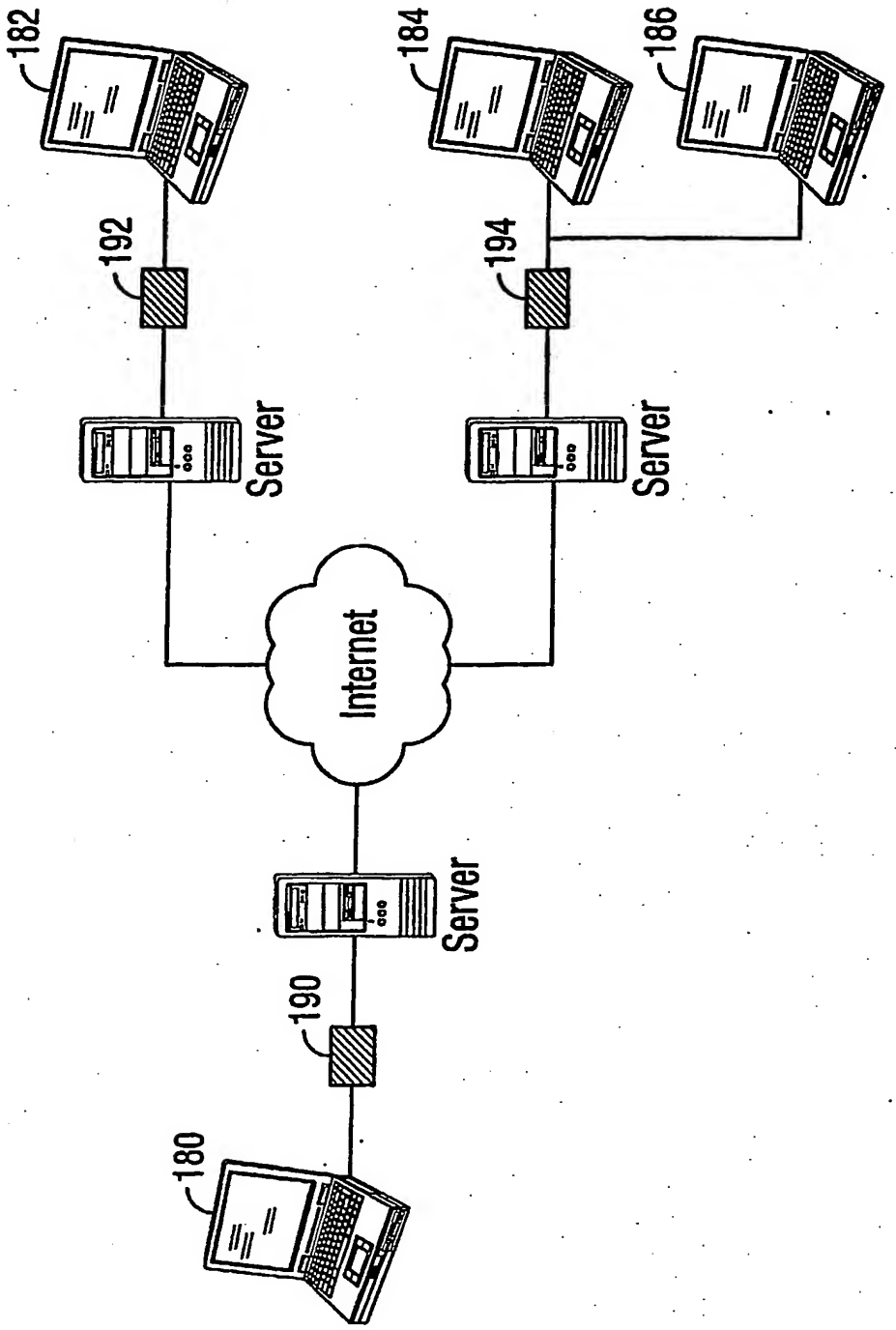


FIG. 14